Section C - Description/Specifications/Statement of Work

Statement of Work (SOW) for Cybersecurity Modeling, Simulations, Assessments, and Analysis

1.0 INTRODUCTION

1.0.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for and is limited to NSWCPD, (b)(6) , which is responsible for Cybersecurity Modeling, Simulations, Assessments, and Analysis of shipboard Naval Control System (NCS) networks, including but not limited to Hull Mechanical & Electrical (HM&E) systems. Efforts within these Cybersecurity specialty areas include design and development of Modeling & Simulations (M&S) and Model-Based Systems Engineering (MBSE) tools to evaluate the Cybersecurity posture of HM&E and other connected systems and maintain Situational Awareness of the impacts associated with Cybersecurity compromises, as well as decision aids to assist engineers with implementing Cybersecure design practices.

1.0.2 This Task Order is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied.

1.0.3 Government / Contractor Relationship

(a) The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Task Order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

(b) The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

(c) Contractor personnel under this Task Order shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

(d) Employee Relationship:

1) The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

2) Rules, regulations, directives, and requirements that are issued by the U.S. Navy and NSWCPD under its responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

(e) Inapplicability of Employee Benefits: This Task Order does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

(f) Notice. It is the Contractor's, as well as the Government's, responsibility to monitor Task Order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1)The Contractor should notify the Contracting Officer in writing within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication involved in the conduct; and the estimate in time by which the Government must respond to this notice to minimize cost, delay, or disruption of performance.

2) The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:
(i) Confirm the conduct is in violation and when necessary direct the mode of further performance,
(ii) Countermand any communication regarded as a violation,
(iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or
(iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

1.1 BACKGROUND

The Hull, Mechanical, and Electrical (HM&E) Cybersecurity branch of NSWCPD is responsible for providing services to: develop Model-Based Systems Engineering (MBSE) tools to model critical cybersecurity data elements representing HM&E and other connected Naval Control Systems (NCS) and perform simulations to asses cybersecurity risk; evaluate and assess the cybersecurity posture of NCS networks, including their cybersecurity vulnerabilities, susceptibility to threats, physical effects and mission impacts of possible cybersecurity incidents; evaluate and assess the cybersecurity risk of a potential compromise by specific threats; recommend cybersecurity controls and mitigations to improve the cybersecurity posture of NCSs; facilitate Cybersecure system design; recommend system design modifications to improve cybersecurity posture; and maintain Situational Awareness with respect to cybersecurity threats targeting NCSs.

The Navy requires Cybersecure solutions for all of its HM&E Control Systems, as well as the systems that monitor, protect, and evaluate those systems, such as those systems under the responsibility of NSWCPD (b)(6) . Cybersecure solutions necessitate the satisfaction of requirements in adherence and compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs). Secure-system configuration and hardening entails Assured Compliance Assessment Solution (ACS) vulnerability assessments, anti-virus (AV) scanning, and certifying-activities to demonstrate and prove a system's capability and reliability within a secure environment.

In addition to the development of Cybersecure solutions, the Navy also requires that all applicable systems be certified and accredited in accordance with the Risk Management Framework (RMF). Certification & Accreditation (C&A) also applies to the Information Technology (IT) information systems, artifacts, and relevant data that are generated by a system-lab-owner (i.e. Information Systems Security Engineer (ISSE)/Information System Owner (ISO) who facilitates C&A via Naval Sea Systems Command (NAVSEA) and Operations Designated Accredited Authority (ODAA); RMF requires the monitoring and maintenance/sustainment of the security posture of the IT systems. Along with the certifying activities, the Navy requires validation of developed capabilities so that they can obtain Authorization to Operate (ATO). Assess & Authorize (A&A) packages must be reviewed and verified prior to issuance of ATOs to ensure complete compliance with RMF.

1.2 SCOPE OF WORK

This Task Order is to support NSWCPD, limited to (b)(6) , in its development of tools to support Cybersecurity M&S, MBSE, analysis, and assessments, as well as, integration with other efforts to maintain situational awareness and implement Cybersecure system design practices. The Contractor shall provide engineering and technical services to support all activities associated with analyzing the Cybersecurity Posture of NCSs, Modeling & Simulations (M&S), Vulnerability Analysis, Threat Analysis, Risk Assessments, recommending and evaluating Security Controls and Mitigations, and finally Structured Data Modeling and Data Analytics. Tasks include development and testing of software and hardware solutions for cybersecurity, design and implementation of advanced risk analysis techniques and systems engineering analysis, development and evaluation models of NCS, mission, and cybersecurity concepts, and performing cybersecurity risk assessments, comparing, verifying, and validating cybersecurity risk assessment processes and results, and finally installation and configuration of cybersecurity software and hardware solutions at alternate hosting sites identified by US Navy resource sponsors.

The Contractor shall support NSWCPD efforts in the following engineering and technical areas:

1.2.1 Software Development

1.2.2 Testing and Integration

1.2.3 Data Modeling

1.2.4 Information Extraction

1.2.5 Cybersecurity Incident Response

1.2.6 Navy Cyber Security Workforce (CSWF)

1.2.7 Technical Writing and Documentation

2.0 APPLICABLE DOCUMENTS

2.1 DoD Instruction 8510.01, Subj: Risk Management Framework (RMF) for DoD Information Technology (IT) dated 12 March 2014 takes effect per NAVSEA guidance.

2.2 DON CIO Memo 01-09, Information Assurance Policy for Platform Information Technology dated 30 Jan 2009.

2.3 NAVSEAINST 9400.2, Implementation of Naval Sea Systems Command (NAVSEA) Afloat Information Assurance (IA) Governance and Guidance dated 18 Aug 10

2.4 DoDD 8500.01x, Information Assurance

2.5 DoDI 8500.2x, Information Assurance Implementation

2.6 DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) dated 28 Nov 2007.

2.7 DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management.

2.8 DoD8570.01-M, Information Assurance Workforce Improvement Program and as migrated to DoDD 8140.

2.9 NIST 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

2.10 Navy Certification Agenda Qualification Standards and Registration Guidebook.

2.11 Navy Authorizing Official and Security Control assessor Risk Management Framework Process Guide (RPG), Version 1, 31 August 2015.

2.12 OPNAVINST 5239.1D, Navy Cybersecurity Program, 22 March 2016.

2.13 CARDEROCKDIVINST 5239.6B, Use of portable electronic devices (PEDs) at the Naval Surface Warfare Center, Carderock Division (NSWCCD) dated 9 July 2010.

2.14 DON-IT Acceptable Use Policy Memorandum, dated 12 FEB 2016

These documents can be referenced at:

Link to AnA News You Can Use documents: https://navsea.navy.deps mil/hq/00i/ia/Pages/default1.aspx

DDCIO(N) RMF portal: https://portal.secnav navy mil/orgs/OPNAV/N2N6/DDCION/N2N6BC4/RMF/SitePages/Home.aspx

RMF Templates:https://portal.secnav.navy.mil/orgs/OPNAV/N2N6/DDCION/N2N6BC4/RMF/SitePages/Home.aspx

The Contractor shall reference and utilize the latest version available when performing tasks within this SOW.

3.0. REQUIREMENTS

3.1 Cybersecurity System Software Development Support:

3.1.1 The Contractor shall provide software lifecycle support following the NSWCPD System Engineering Process (SEP) with applicable Capability Maturity Model Integrated (CMMI) and Institute of Electrical and Electronics Engineers (IEEE) standards and specifications.

3.1.2 The Contractor shall develop and/or modify control system cybersecurity software and hardware solutions including but not limited to: modeling and simulations tools, vulnerability assessment tools, threat analysis tools, risk assessment tools, situational awareness tools, and forensics tools.

3.1.3 The Contractor shall develop and/or modify computer code in the following languages: C/C++, C#, Java, Visual Basic, MATLAB, and Labview as well as other related high-level programming languages. The Contractor shall support a range of Integrated Development Environments (IDEs) including but not limited to Visual Studio and Eclipse.

3.1.4 The Contractor shall develop and/or modify Human-Machine Interfaces (HMIs) and/or Graphical User Interfaces (GUIs) using applicable development tools.

3.1.5 The Contractor shall use networked and IP-based systems and knowledge of network protocols including TCP/IP (Transmission Control Protocol/Internet Protocol) and UDP (User Datagram Protocol).

3.1.6 The Contractor shall use and apply knowledge of Industrial Control Protocols including but not limited to: Modbus, VME bus, and other common Industrial Control protocols and their variants.

3.1.7 The Contractor shall develop software change packages and artifacts and present at peer reviews.

3.1.8 The Contractor shall use software issue reporting and tracking databases/tools.

3.1.9 The Contractor shall develop, modify, and use virtualized (e.g. Xen, VMWare, etc.) environments.

3.1.10 The Contractor shall support development of graphical user interfaces, visuals, and output reports that display data, metrics, and other supporting information about the cybersecurity posture of NCSs.

3.1.11 The Contractor shall develop databases utilizing products such as but not limited to; Microsoft Access, Structured Query Language (SQL), Comma Separated Values (CSV), Resource Description Framework (RDF), Web Ontology Language (OWL), and Franz, Inc. AllegroGraph.

3.1.12 The Contractor shall design software, including standalone applications, webpages, and databases, to meet cybersecurity and information assurance requirements, and improve the security features of existing applications to be in compliance with the latest (NIST) standards.

This includes:

3.1.12.1 Project planning and consultation with NSWCPD

3.1.12.2 Resource planning and scheduling

3.1.12.3 Software Requirements Documentation

3.1.12.4 Configuration Management (CM) Documentation

3.1.12.5 Application Consolidation

3.1.12.6 Migration

3.1.12.7 Retirement

3.2 Control Systems Cybersecurity Testing and Integration Engineering Services:

3.2.1 The Contractor shall develop software unit and system tests in order to demonstrate that computer programs satisfy all requirements.

3.2.2 The Contractor shall perform software security analysis on developed and provided software baselines.

3.2.3 The Contractor shall perform static and/or dynamic analysis on source code for developed and provided software baselines.

3.2.4 The Contractor shall develop, plan, schedule, and execute test plans and test procedures for computer programs and hardware.

3.2.5 The Contractor shall document issues, faults, or deficiencies found during software and hardware testing, troubleshoot issues, identify root cause, and provide solutions to enable testing to continue.

3.2.6 The Contractor shall provide remote troubleshooting assistance to onsite representatives.

3.2.7 The Contractor shall perform Configuration Management (CM) of all developed software, hardware, and documentation in accordance with the approved SEP Configuration Management Plan (CMP) using software version control tools, including but not limited to Git, Telelogic DOORS, Sharepoint Excel, Word Access, and Project.

3.2.8 The Contractor shall provide hardware and software administration, maintenance, and disaster recovery support.

3.2.9 The Contractor shall provide cybersecurity support services to facilitate ongoing authorization efforts.

3.2.10 The Contractor shall maintain technical software development skills to contribute to new software development efforts and to assist with advising software developers on fixes for any identified issues, faults, or deficiencies found during testing.

3.2.11 The Contractor shall develop software and/or hardware installation plans with input from external supporting commands and technical authorities.

3.2.12 The Contractor shall develop, maintain, and configuration manage software and hardware installation procedures, instructions, notices, and Standard Operating Procedures (SOPs).

3.2.13 The Contractor shall develop Engineering Change Proposal (ECP) packages for cybersecurity systems.

3.2.14 The Contractor shall provide engineering services that include development and maintenance in support of hardware and software technical documentation and requirements.

3.2.15 The Contractor shall provide engineering services that include development and maintenance in support of technical data packages (TDPs).
3.2.16 The Contractor shall utilize automated software testing and integration tool suites including but not limited to: JUnit, Sonarqube, Jenkins, and FindBugs.

3.3 Data Modeling in support of Cybersecurity M&S:

3.3.1 The Contractor shall work with stakeholders to define and decompose requirements for a logical data model to capture Navy afloat and undersea integrated systems. Stakeholders may include program office personnel, US Fleet Cyber Command, National Security Agency, as well as NAVSEA, NAVAIR, NAVFAC, and SPAWAR headquarters organizations.

3.3.2 The Contractor shall establish methodologies for capturing and managing data associated with complex integrated HM&E, Combat, Navigation, and C4I systems.

3.3.3 The Contractor shall develop and/or modify logical data models enabling and enforcing concordance and mapping between system, subsystem, interface, mission thread, process, and other data sets.

3.3.4 The Contractor shall develop and/or modify logical data models that store data elements to support data call responses, information flow analyses, operations analysis, performance evaluations, mission thread analyses, cybersecurity assessments, and engineering change evaluations.

3.3.5 The Contractor shall develop and/or modify data models and/or simulations to capture the data shared between NCS devices and sub-systems, as well as the semantic representations of the physical and/or mission effects associated with data shared between NCS devices and sub-systems.

3.3.6 The Contractor shall develop and/or modify data models and/or simulations to capture the physical effects and mission impacts produced by operational functionality of NCS devices and sub-systems, malfunctions of NCS devices and sub-systems, and/or complete operational failure of NCS devices and sub-systems.

3.3.7 The Contractor shall develop and/or modify data models and/or simulations to capture the attributes of adversarial and non-adversarial threats targeting NCSs.

3.3.8 The Contractor shall work with stakeholders as required to conduct systems and data research in support of development and sustainment of data models and/or simulations.

3.3.9 The Contractor shall research the application of M&S techniques as applicable to NCS and/or cybersecurity, as well as specific data models, to acquisition, engineering, and logistics support applications and develop associated data management and reporting capabilities.

3.3.10 The Contractor shall support development of requirements for and support the application of a collaborative data modeling environment for both stand-alone users and remote access users at multiple classifications.

3.3.11 The Contractor shall utilize Knowledge Representation & Reasoning (KR&R) tools and techniques to support development, modification, and application of data models linking NCS concepts to critical cybersecurity data elements and mission concepts

3.3.12 The Contractor shall modify and use databases utilizing products such as but not limited to: Microsoft Access, Structured Query Language (SQL), Comma Separated Values (CSV), Resource Description Framework (RDF), Web Ontology Language (OWL), and Franz, Inc. AllegroGraph.

3.4 **Information Extraction to Support Cybersecurity M&S:**

3.4.1 The Contractor shall develop Natural Language Processing (NLP) techniques to identify cybersecurity-critical data elements from technical documents, extract the data elements, and map them to existing and new data models.

3.4.2 The Contractor shall develop NLP techniques to extract cybersecurity-critical data elements from Open-Source Intelligence (OSINT) documents, including but not limited to public-facing web repositories, and map the extracted data elements to existing and new data models.

3.4.3 The Contractor shall develop software to automatically extract cybersecurity-critical data elements from structured data sources, including but not limited to spreadsheets, tables, and markup languages such as eXtensible Markup Language (XML) or System Modeling Language (SysML), and map the extracted data elements to existing and new data models.

3.4.4 The Contractor shall develop Image Processing techniques to extract cybersecurity-critical data elements from technical diagrams and map the extracted data elements to existing and new data models.

3.4.5 The Contractor shall develop Image Processing techniques to extract cybersecurity-critical data elements from images of text in formats such as PDF, PNG, JPEG, or other format for storing image data, then map extracted data elements to existing and new data models.

3.4.6 The Contractor shall develop and/or apply Machine Learning techniques to identify cybersecurity-critical data elements from technical documents, images, and other data sources, producing output for automated Information Extraction algorithms.

3.5 **Cybersecurity Assessments, Evaluations, and Analysis:**

3.5.1 The Contractor shall develop methods for evaluating and measuring threats targeting NCSs, vulnerabilities of NCSs and components, impacts of threats on NCSs, and effective security mitigations and controls that should be employed in order to protect NCSs, including but not limited to automatic methods.

3.5.2 The Contractor shall conduct Cybersecurity Risk Assessments of NCS networks.

3.5.3 The Contractor shall analyze critical Cybersecurity data elements to evaluate the vulnerabilities of NCSs, NCS components, and NCS subsystems, their susceptibility to cybersecurity threats, and applicable recommendations of security mitigations and controls.

3.5.4 The Contractor shall develop and/or utilize Machine Learning tools and techniques to support automatic cybersecurity assessments.

3.5.5 The Contractor shall utilize Knowledge Representation & Reasoning (KR&R) tools and techniques, including but not limited to development of rulesets and queries, to support automatic cybersecurity assessments.

3.5.6 The Contractor shall review, analyze, and create a means of modeling and simulating Failure Mode and Effects Analysis (FMEA), Failure Modes, Effects and Criticality Analysis (FMECA), and Failure Modes & Impacts Criticality Analysis (FMICA).

3.6 **Cybersecurity Incident Response:**

3.6.1 The Contractor shall recommend Incident Response plans or specific actions based on their evaluation of relevant data, including but not limited to: incident reports, outputs of Intrusion Detection/ Perimeter Security (ID/PS) systems, network and host activity logs, and outputs of forensic analysis systems.

3.6.2 The Contractor shall execute remediation activities to address Cybersecurity incidents in accordance with the Incident Response plans pertaining to specific systems, including but not limited to Cybersecurity software tools.

3.7 Cybersecurity Workforce (CSWF) Support:

3.7.1 The Contractor shall provide technical services in support of delivering cyber-secure systems and solutions including the development and submittal of Risk Management Framework (RMF) risk assessments, implementation of DoD secure system configuration and hardening, requirements identified in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs), Assured Compliance Assessment Solution (ACAS) vulnerability assessments, anti-virus (AV) scanning, Standard Engineering Process (SEP) artifacts, and other supporting documentation required for certifying and maintaining afloat, RDT&E, and/or enterprise platforms.

3.7.2 The Contractor shall develop RMF Assess & Authorize (A&A) package documentation in accordance with DoD/NAVSEA directives, which includes the following components: Platform IT (PIT) Determination package documentation, System Categorization Form, Information System Continuous Monitoring Strategy (ISCM), Security Plan (SP), Step Concurrence forms, Plan of Actions and Milestones (POA&M), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment Report (RAR), Security Authorization Package, CYBERSAFE Certification, Package Endorsement Letters, and any additional administrative/technical resources required for submission.

3.7.3 The Contractor shall ensure RMF A&A package is submitted to the certification authority (CA) in sufficient time for review and operational cybersecurity risk recommendation to obtain Designated Accrediting Authority (DAA) authorization decision prior to operations or tests on a live network (i.e. LBES or shipboard).

3.7.4 The Contractor shall develop, maintain, and execute all IA related tasks and duties in accordance with regulations to include the development and execution of RMF Program to Plan of Action and Milestone (POA&M) or Security Technical Implementation Guide (STIG).

3.7.5 In accordance with RMF, the Contractor shall monitor and maintain the security posture of IT systems to include patching, implementing STIGs, analyzing network traffic, and applying new physical security measures.

3.7.6 Develop and/or test new and existing security features to be implemented into the control system operating environment and/or software.

3.8 Technical Writing and Documentation:

3.8.1 The Contractor shall develop, evaluate, update, and provide feedback on technical documentation and other logistics products such as technical manuals, system diagrams, system drawings, signal flow diagrams, allowable parts list, preventative maintenance cards, and engineering operational and casualty procedures.

3.8.2 The Contractor shall assist engineers with compiling data into test plans and reports.

3.8.3 The Contractor shall assist engineers with technical documentation revisions.

3.8.4 The Contractor shall assist engineers with developing presentations for Program Reviews.

3.9 Information System Security Manager (ISSM) Support:

3.9.1 The Contractor shall ensure that information systems used in supporting task requirements comply with initial and ongoing information systems security requirements in accordance with, FIPS Publication 200, Minimum Security Requirements of Federal Information Systems.

3.9.2 The Contractor shall ensure that information systems used to support a specific task meet the minimum security requirements as defined in FIPS Publication 200 through the use of security controls, in accordance with the NIST Special Publication 800 – 53, Recommended Security Controls for Federal Information Systems, As Amended. This includes preparing all required documentation for the compliance process, including a security plan, risk assessments, contingency and contingency test plans, a configuration management plan, system test and evaluation reports, security certification, and an accreditation package.

3.10 Information System Security Engineer (ISSE) Support:

3.10.1 The Contractor shall provide analysis of cybersecurity requirements and potential design solutions, providing guidance and direction related to security technologies, performing analysis on cybersecurity collected data and test results, identifying and implementing cybersecurity design, and preparing and maintaining engineering and security related documentation.

3.10.2 The Contractor shall perform and provide vulnerability assessment results and recommendations to NSWCPD.

3.10.3 The Contractor shall assess know systems vulnerabilities and verify system hardening and patching activities to ensure compliance with the most current applicable Security Technical Implementation Guides (STIGs)/Security Requirements Guides (SRGs) and related checklists.

3.10.4 The Contractor shall document, implement and prioritize patching requirements across applicable system components.

3.10.5 The Contractor shall provide support for the development and testing of patches to fix vulnerabilities in Windows, RHEL operating systems and associated applications.

3.10.6 The Contractor shall provide assistance in conducting cybersecurity audits to ensure appropriate implementation and compliance of the security posture.

3.10.7 The Contractor shall perform system security engineering and test efforts associated with implementation of security controls on networking devices, databases, operating systems, hardware and software components.

3.10.8 The Contractor shall develop vulnerability reports and investigation impact, resolution and verification of security vulnerabilities and patches as well as performing deep dive and impact analysis into failed patch deployments.

3.10.9 The Contractor shall provide regular reporting on patch management program and overall operation status of patch compliance.

3.11 NAVY CYBERSECURITY WORKFORCE (CSWF) REQUIREMENTS

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, and SECNAV 5239.2, DON IAWF Management Manual to support the Cybersecurity/IAWF Program, Contractors performing IA functions must be designated as a member of the Cybersecurity\IA Workforce and meet qualification requirements for their duties, which may include both an IA baseline certification and operating system (OS)/Computing Environment (CE) certification requirement per below instructions: Contractors performing Cybersecurity/IA functions must meet the minimum IA baseline certification prior to being engaged as defined in the CSWF Matrix below.

Contractor personnel agree as a "condition of employment" to obtain (and maintain) the appropriate certifications and continuing profession education requirements for their Cybersecurity/IAWF position. Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570.01M and SECNAV M-5239.2. The Contractor is responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570.01M and the Computing Environment/Operating System (CE/OS) certifications in accordance with the CSWF Matrix below.

Upon hire all Contractor personnel assigned to the IAM/IAT Level I-III position (as appropriate) shall sign the Information System Privileged Access Agreement and Acknowledgement of Responsibilities statement. Cybersecurity/IA Workforce labor categories are identified herein. The Contractor shall ensure that personnel have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including: DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M Appropriate operating system certification for information assurance technical (IAT) positions as required by DoD 8570.01-M.

The Contractor shall provide the current information assurance certificates/documentation supporting IA certification and current status of personnel performing Cybersecurity/IA duties. Baseline and Operating System (OS) Certification requirements listed in the CSWF Matrix must be met and are a condition of hire. The Contractor shall ensure that cybersecurity/IA Contractor personnel are appropriately certified and maintain current Continuing Professional Education (CPE) requirements as a condition of employment. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

Information assurance contractor training and certification. This Task Order includes information assurance functional services for DoD information systems, and requires appropriately cleared Contractor personnel to access a DoD information system to perform Task Order duties, the Contractor is responsible for providing to the contracting officer: A list of information assurance functional responsibilities for DoD information systems by category (e.g., technical or

management) and level (e.g., computing environment, network environment, or enclave); The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

After Task Order award, the Contractor is responsible for ensuring that the certifications and certification status of all Contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked. The responsibilities specified apply to all DoD information assurance duties supported by a Contractor, whether performed full-time or part-time as additional or embedded duties, and when using a DoD Contract, or a Task Order, or agreement administered by another agency.

BASELINE CERTIFICATION-The baseline certification is a security certification and is required for all IA members (all IAT and IAM levels) of the Cybersecurity Workforce/IA Workforce. Contractors must have a baseline certification prior to performing any IA duties and is a condition of hire.

COMPUTING ENVIRONMENT (CE) CERTIFICATION- All IAT levels require Computing Environment certification for the appropriate operating system they support and in which access is granted. These certifications are typically vendor specific and depend on the supported hardware or operating system. (i.e., Microsoft computing environment requires MCITP-SA and Linux computing environment requires LINUX+).

Table 1- Cybersecurity WorkForce (CSWF) Certification Matrix

Task Area	Labor Category	Specialty Code	Proficiency Level	Baseline Qualification	Operating System/ Computing Environment(OS/CE) Qualification	Continuing Professional Education (CPE) Reqt's
3 1	Manager, Program/Project ECT II	75	Intermediate/ Journeyman	Bachelor Degree from accredited University	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer IV	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer – Systems IV	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer, Computer IV	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer, Computer I	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or	Directed by the Privileged Access Agreement	**40 CPEs annually**

				NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate		
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer, Computer II	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Analyst – Computer Systems II	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Analyst – Computer Systems III	62	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer II	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 1, 3 2, 3 3, 3 4, 3 5, 3 6	Engineer – Systems II	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CCNA or CAP or Security + (CE) or CNSSI 4012-4016 Certificate or NDU CISO certificate or NEC 2780 or 2779 or 2781 or CISS Certificate	Directed by the Privileged Access Agreement	**40 CPEs annually**
3 3, 3 6	Computer Operator II	46	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI or NTSSI 4015 or	Directed by the Privileged Access Agreement	**40 CPEs annually**

				4016 GSEC or Security + (CE) or SSCP		
3 9	Information Systems Security Manager II (ISSM)	72	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012 Certificate; CASP or CAP or Security+ or Program Management Professional	Directed by the Privileged Access Agreement	**40 CPEs annually**

CONTINUING PROFESSIONAL EDUCATION (CPE) REQUIREMENTS- As technology continuously advances; nearly all certifications expire or have continuing professional education (CPE) requirements. Both the baseline certifications and computing environment certifications may require continuous education. The vendor requirements state whether the certifications require continuous education. Continuing Professional Education (CPE) requirements are not a direct contractor cost to the Government. The Contractor is responsible for meeting the qualification requirements for all positions on the Task Order in the Cybersecurity/IAWF matrix and should not invoice the Government for training, certification tests, or continuing profession education requirements.

Ensure that if you have any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce you must identify the required security, certifications, education, and training for EACH labor category. Reference DFARS Clause 252.239-7001, DoD 8750.01-M "Information Workforce Improvement Program", DoD 8140.01 "Cyberspace Workforce Management", and SECNAV M-5239.2 "Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual.

4. DATA REQUIREMENTS.

All Contracts Data Requirements Lists (CDRL) shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR. The Contractor agrees that the US Navy owns all rights to Intellectual Property (IP) created under this Task Order, including but not limited to algorithms, source code, data, and documentation. The Contractor maintains no licensing or re-use rights for IP created under this Task Order.

DFARS 252.204-7000 Disclosure of Information.

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this Task Order or any program related to this Task Order, unless—

(1) The Contracting Officer has given prior written approval; or

(2) The information is otherwise in the public domain before the date of release.

(b) Requests for approval shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 45 days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement in each subcontract under this Task Order. Subcontractors shall submit requests for authorization to release through the prime Contractor to the Contracting Officer.

4.1 Contract Status Report (CDRL A001)

4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.

4.1.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.2 Travel Report (CDRL A002)

4.2.1 This report shall reflect both prime Contractor and Subcontractor data if applicable at the same level of detail.

4.2.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.3 Contractor's Personnel Roster (CDRL A003)

4.3.1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR. This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.

5. SECURITY REQUIREMENTS

5.1 An active SECRET Facility Clearance (FLC) is required for performance at the time of award for this Task Order. There is no safeguarding requirement required. The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this Task Order, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWC PD, Security Office, Code 105.

The Prime Contractor shall:

(1) Forward copies of DD254s provided to Subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.

(2) Direct the Subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.

(3) Submit the Subcontractor's request for public release through the technical point of contact identified on the DD 254.

5.2 The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems to include but not limited to DoD Cyber-Awareness Challenge, Operations Security (OPSEC), NAVSEA Counterintelligence Training, Privacy and Personally Identifiable Information (PII) Awareness Training, Controlled Unclassified Information training NAVSEA Physical Security training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the Task Order.

5.3. Personnel assigned to this contact will require access to SIPRnet. Contractor must receive a NATO security briefing and derivative classification training prior to access from the Contractor's Facility Security Officer (FSO). The FSO shall ensure all personnel receive an initial and annual NATO security briefing along with initial and biennial derivative classification training during the life of this Task Order. Evidence of completion, training certificates or equivalent, shall be provided to the Government Contracting Agency GCA no later than the individual's start date. The Contractor will not use the SIPRnet for anything except that which is required for this Task Order.

5.4. Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors must bring the ID that is listed on the I-9 form to the NSWCPD Security Officer at the time of badge request to verify U.S. citizenship.

5.5. A T1 investigations will be completed on any contractor that does not have a favorable adjudicated investigation in JPAS and is requesting swipe/non-swipe access to our buildings in excess of 120 days. Any contractor that has unfavorable information that has not been favorably adjudicated by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge.

5.6. Within 30 days after contract award, the Contractor shall submit a list of all Contractor personnel, including subcontractor employees, who will have access to DON information systems and/or work on-site at one of the NSWCPD sites to the appointed Contracting Officer Representative (COR) via email. The Contractor shall provide each employee's first name, last name, contract number, the NSWCPD technical code, work location, whether or not the employee has a CAC card and/or swipe card, the systems the employee can access (i.e., NMCI, RDT&E), and the name of the Contractor's local point of contact, phone number and email address. Throughout the period of performance of the contract, the Contractor shall immediately provide any updated information to the COR when any Contractor personnel changes occur including substitutions or departures.

5.7. Once contract performance is complete the contractor shall return the CAC card to the COR. If the contractor will be performing services for NSWCPD under a different DoD issued contract, the COR may authorize the contractor to retain the CAC card until those services are complete. Notification to the NSWCPD Security Office must be provided via by the COR via an email with contractor's name and the new contract number.

6. PLACE OF PERFORMANCE

6.1 Performance will occur at NSWCPD.

6.1.1 The specific location(s) will be provided at time of award of the Task Order. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.2 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Task Order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

6.1.3 Early Dismissal and Closure of Government Facilities

When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the Task Order for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Task Order. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Task Order period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allow ability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

7. TRAVEL (CDRL A002)

The Contractor may be required to travel from the primary performance location when supporting this requirement. For estimating purposes, the following annual travel information is provided; estimates are for two people per trip. Destinations, duration, and number of trips are subject to change.

DESTINATION:	Number of Days/Trip	Total Number of Trips
Washington, DC	1	10
Norfolk, VA	7	6
San Diego, CA	7	6
Everett, WA	0	0
Yokosuka, Japan	0	0
Mayport, FL	0	0
Pascagoula, MS	0	0
Bath, ME	0	0
Honolulu, HI	5	3
Rota, Spain	0	0
Orlando, FL	0	0
Annapolis, MD	0	0
Leesburg, VA	0	0
New Orleans, LA	0	0
Milwaukee, WS	0	0
Cincinnati, OH	0	0

The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR and Contracting Officer before travel occurs. Approval may be via the Technical Instruction (TI). In accordance with the TI instructions, before initiating any travel, the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 TRAVEL COSTS (NAVSEA) (OCT 2018) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

Travel Costs

The Government shall reimburse the Contractor and its Subcontractors at a reduced reimbursement rate from the current “maximum per diem” rates for lodging, meals, and incidentals, referenced in FAR 31.205-46(a)(2), for any employees, purchased labor, consultants, etc. assigned to a temporary duty station (TDY) in excess of 30 days in one location. This applies to both CONUS and OCONUS travel. The current “maximum per diem” rates are set forth in the

(i) Federal Travel Regulations for travel in the Continental United States;

(ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and

(ii) Department of State (DOS) prescribed rates for foreign overseas locations.

When proposed travel is in excess of 30 consecutive days, but less than 180 consecutive days, the Government shall limit reimbursement of contractor (and subcontractor) travel costs, on a flat rate basis, to 75 percent of the per diem rate for the TDY locality at the time of travel (lodging, meals, and incidentals) for each full day, long-term TDY of 31 to 180 days. For travel lasting in excess of 180 days, the Government shall limit reimbursement of contractor (and subcontractor) travel costs, on a flat rate basis, to 55 percent of the per diem rates of the TDY locality at the time of travel for each full day.

8.0 GOVERNMENT FURNISHED PROPERTY

Government Furnished Property (GFP) will be provided (CDRL 005).

9.0 GOVERNMENT FURNISHED INFORMATION

N/A at this time.

10. PURCHASES

Only items directly used and incidental to the services for this Task Order, and for work within the scope of the Statement of Work, shall be purchased under the Other Direct Cost (ODC) line items. Individual purchases above $10,000.00 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR). It shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

11. PERSONNEL

11.1 **Personnel Requirements.**

All persons proposed in key and non-key labor categories shall be U.S. citizens holding at least a current SECRET clearance at the time of Task Order award. All persons must adhere with the requirements in the CSWF matrix in Paragraph 3.11 of this Statement of Work.

Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this Task Order in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime Contractor. This overtime premium amount shall equal the prime Contractor's unburdened premium OT labor costs plus the Subcontractors' fully-burdened premium OT labor costs.

The level of effort for the performance of the resultant Task Order is based on the following labor categories and total hours for all years:

Title (Key Personnel)	**Site**	**Hours**	**OT HRs**	**Resumes Req**
MANAGER, PROGRAM/PROJECT II (MANP2)	Contractor	8,160	576	1
ENGINEER IV (E4)	Government	19,200	2,112	2
ENGINEER, SYSTEMS IV (ESY4)	Government	24,960	2,496	3
ENGINEER, COMPUTER IV (EC4)	Government	24,960	2,496	3
ANALYST, COMPUTER SYSTEMS III (14103)	Government	17,280	1,728	2
INFORMATION SYSTEM SECURITY MANAGER II (ISSM2)	Government	9,600	192	1
Title (Non-Key Personnel)				
ADMINISTRATIVE ASSISTANT (01020)	Government, Contractor	2,920	192	0
ENGINEER II (E2)	Government	9,600	960	0
ENGINEER, SYSTEMS II (ESY2)	Government	9,600	960	0
ENGINEER, COMPUTER I (EC1)	Government	1,920	192	0
ENGINEER, COMPUTER II (EC2)	Government	9,600	960	0
ENGINEER, ELECTRICAL I (EE1)	Government	1,920	192	0
COMPUTER OPERATOR II (14042)	Government	7,680	768	0
ANALYST, COMPUTER SYSTEMS II (14102)	Government	9,600	960	0
SPECIALIST, CONFIGURATION MGMT II (SCM2)	Government	5,760	576	0
TECHNICAL WRITER, SUPERVISORY(TECW)	Contractor	2,400	0	0

11.1.1 Key Personnel

The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Task Order in accordance with Clause 52.237-3 Continuity of Services (Jan 1991) in the basic Seaport NxG contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

In accordance with C-237-H002 Substitution of Personnel, the following labor categories are designated as the target Key Personnel for this Task Order. Additional non-key personnel may also be utilized in these labor categories as tasking requires. Resumes will be submitted for each category in the quantities indicated by the key category description. Target and/or minimum qualifications are listed below for each education and work experience qualifications for each key personnel labor category. The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for task areas

C.1-C.7 in this Statement of Work.

The Contractor shall provide individuals to fill the key positions identified below:

MANAGER, PROGRAM/PROJECT II (MANP2) (1 Resume required):

Minimum Education: Individual should possess a Bachelor's of Science Degree in Engineering or Computer Science from an accredited college or university.

Target Experience: Ten (10) years' experience. The experience should include experience in a management capacity with responsibilities for major project or program level management of Contractors/subordinates. Relevant experience in a management capacity with responsibilities for financial management, tracking and fiscal oversight of program funding is preferred. Working knowledge of the Naval Sea System Command, Naval Surface Warfare Center and Fleet organizations is desired. In lieu of the education requirement, individuals should have fifteen (15) years of relevant experience in the program management and program oversight of Control System/Information System or other technical equipment, systems or programs for the U.S. Navy.

ENGINEER IV (E4) - M&S / MBSE TOOLS DATA SCIENTIST (2 Resumes required):

Minimum Education: Bachelor of Science (BS) Degree in Mechanical Engineering or Electrical Engineering or Computer Engineering from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Target Experience:

- Seven (7) years of professional experience within industry as a systems engineer, electrical, computer and/or electronics engineer
- Two (2) years of professional experience in MATLAB, SIMULINK, R, Python, or other analytical programming language
- One (1) year of experience developing or applying Machine Learning and/or Knowledge Representation & Reasoning (KR&R) tools, techniques, and/or algorithms
- One (1) or more years of experience developing or applying Semantic Web technologies including but not limited to: Web Ontology Language (OWL) and Resource Description Framework (RDF)
- Two (2) years of professional experience developing software using one or more high-level languages such as C/C++ or Java.
- One (1) or more years of experience developing or applying Semantic Web technologies including but not limited to: Web Ontology Language (OWL) and Resource Description Framework (RDF)

ENGINEER, SYSTEMS IV (ESY4) - M&S / MBSE SYSTEMS ENGINEER (3 Resumes required):

Minimum Education: Bachelor of Science (BS) Degree in Mechanical Engineering or Electrical Engineering or Computer Engineering from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Target Experience:

- Three (3) years of professional experience within industry as a systems, electrical, and/or electronics engineer, or in MBSE and/or M&S
- Two (2) years of professional experience troubleshooting hardware/software systems
- One (1) year of professional experience troubleshooting network based systems

ENGINEER, COMPUTER IV (EC4) - M&S / MBSE TOOLS SOFTWARE ENGINEER (3 Resumes required):

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science.

Target Experience:

- Three (3) years of professional experience developing software using one or more high-level languages such as C/C++ or Java.
- One (1) year of professional experience designing and/or analyzing software architectures
- Two (2) years of professional experience developing software for web or distributed architecture applications
- One (1) or more years of professional experience developing and/or using Semantic Graph Database technologies such as Franz, Inc. AllegroGraph, Neo4j, Stardog, or similar, or developing and/or using Relational Database technologies such as SQL, or flexible-schema Database technologies such as NoSQL
- One (1) or more years of professional experience developing Natural Language Processing (NLP) algorithms and/or using NLP software tools such as the GATE Framework or Natural Language Toolkit (NLTK).

ANALYST, COMPUTER SYSTEMS III - CYBERSECURITY ENGINEER / CYBERSECURITY ANALYST (14103) (2 Resumes required):

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science, or a Cyber Security related degree from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Target Experience:

- One (1) year of professional experience in cyber security engineering
- One (1) year of professional experience with IT infrastructure, networks, and/or network security CompTIA Security+ Certification or higher level cybersecurity certification, such as (ISC)2 CISSP
- One (1) year of professional experience using vulnerability analysis tools

- One (1) year of professional experience applying and/or using and/or analyzing cybersecurity controls such as intrusion detection systems, intrusion prevention system, firewall configurations, and access control lists
- One (1) year of professional experience maintaining and configuring various operating systems such as Windows, Linux, VxWorks, or other Embedded Operating Systems

INFORMATION SYSTEM SECURITY MANAGER II (ISSM2) (1 Resume required):

Minimum Education: Bachelor Degree from accredited University or CNSSI 4012 certificate or ADQ GA7 or successful completion of at least one of the following military training courses: NEC 2779 (CIN: 1-531-0009) or 3372 or CIN W-3B-1500 (EKMS Manager) or A-4C-1340 (KMI) (or DoD Service equivalent)

Target Experience: Three (3) years of specialized entry level experience in Specialty Area 72 (Information System Security Management)

11.1.2 Non-Key Personnel

Although resumes for "Non-Key Personnel" are not required, offerors must fully demonstrate their ability to provide the non-key personnel listed below who meet the minimum requirements that follow. The Contractor shall certify in their proposal that they have these non-key personnel and provide a statement as to their ability to supply the personnel with the experience required to perform the efforts specified in the Statement of Work. The Contractor shall provide individuals to fill the non-key positions identified below:

SPECIALIST, CONFIGURATION MGMT II (SCM2):

Minimum Education: Bachelor's Degree in any field.

Minimum Experience: Three (3) years of configuration management experience.

ENGINEER II (E2):

Minimum Education: Bachelor of Science (BS) Degree in Mechanical Engineering or Electrical Engineering or Computer Engineering from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Minimum Experience:

- One (1) year of professional experience within industry as a systems, electrical, computer, and/or electronics engineer
- One (1) year of professional experience developing software using one or more high-level languages such as C/C++ or Java.
- One (1) year of professional experience reading and/or creating electrical schematics and/or network diagrams
- One (1) year of professional experience working with hardware/software systems in environments such as NCS, ICS, or warehouse automation

ENGINEER, SYSTEMS II (ESY2):

Minimum Education: Bachelor of Science (BS) Degree in Mechanical Engineering or Electrical Engineering from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Minimum Experience:

- One (1) year of professional experience within industry as a systems, electrical, and/or electronics engineer
- One (1) year of professional experience troubleshooting hardware/software systems in environments such as NCS, ICS, or warehouse automation
- One (1) year of professional experience reading and/or creating electrical schematics and/or network diagrams
- One (1) year of professional experience troubleshooting network based systems

ENGINEER, COMPUTER I (EC1):

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science.

Minimum Experience:

- One (1) year of professional experience developing software using one or more high-level languages such as C/C++ or Java.
- One (1) year of professional experience using IDEs such as Microsoft Visual Studio, Eclipse, NetBeans, or similar to develop, compile, and debug source code
- One (1) or more years of professional experience developing and/or using Relational Database technologies such as SQL, or flexible-schema Database technologies such as NoSQL

ENGINEER, COMPUTER II (EC2):

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science.

Minimum Experience:

- Two (2) years of professional experience developing software using one or more high-level languages such as C/C++ or Java.
- One (1) year of professional experience using IDEs such as Microsoft Visual Studio, Eclipse, NetBeans, or similar to develop, compile, and debug source code
- One (1) or more years of professional experience developing and/or using Relational Database technologies such as SQL, or flexible-schema Database technologies such as NoSQL
- One (1) year of professional experience as a technical and/or programming lead for a software project through the software life cycle, from requirements to design, implementation, deployment, and maintenance.

ENGINEER, ELECTRICAL I (EE1):

Minimum Education: Bachelor of Science (BS) Degree in Electrical Engineering from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Minimum Experience:

- One (1) year of professional experience within industry as a systems, electrical, and/or electronics engineer
- One (1) year of professional experience troubleshooting hardware/software systems in environments such as NCS, ICS, or warehouse automation
- One (1) year of professional experience reading and/or creating electrical schematics and/or network diagrams
- One (1) year of professional experience troubleshooting network based systems

ANALYST, COMPUTER SYSTEMS II (14102):

Minimum Education: Bachelor of Science degree in Computer Science, Electrical Engineering, or Computer Engineering or a Cyber Security related degree from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Minimum Experience:

- Two (2) years of professional experience in cyber security engineering Security+ Certification or CISSP Certification
- One (1) year of professional experience with vulnerability analysis tools
- One (1) year of professional experience maintaining and configuring various operating systems such as Windows, Linux, VxWorks, or other Embedded Operating Systems

COMPUTER OPERATOR II (14042):

Minimum Education: Bachelor's Degree in Computer Information Systems, Computer Science, Computer Engineering, or a related field from an ABET (Accreditation Board for Engineering and Technology) accredited program.

Minimum Experience:

- Three (3) years of professional experience in IT/Help Desk support and asset management
- One (1) year of professional experience maintaining and configuring various Windows operating systems

TECHNICAL WRITER, SUPERVISORY (TECW):

Minimum Education: Bachelor's Degree in any field.

Minimum Experience:

- Three (3) years of professional experience within industry in technical writing and editing.
- One (1) year of professional experience within industry editing technical documentation for US Navy or USCG.

ADMINISTRATIVE ASSISTANT (01020):

Minimum Education: High School Diploma (or GED Equivalent)

Minimum Experience: Three (3) years of professional experience using Word and Excel or other equivalent programs

12.0 NSWCPD ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (ECRAFT) SYSTEM

The contractor agrees to provide supporting accounting system reports, at the Contracting Officer's request, based on the review of the invoice documentation submitted to eCRAFT. This documentation will include reports such as the Job Summary Report (or equivalent), Labor Distribution Report (or equivalent), and General Ledger Detail Report (or equivalent). Supporting labor data provided must include unburdened direct labor rates for each employee and labor category. Cost breakdowns for ODCs, Materials, travel and other non-labor costs must be at the transactional level in sufficient detail so the Government can review allocability to the contract/task order. Indirect costs allocated to direct costs must be shown at the lowest level of detail sufficient to reconcile each indirect rate to the appropriate allocation base.

On invoices containing subcontractor costs, the prime contractor agrees, at the Contracting Officer's request, to attach as supporting documentation all invoices received from subcontractors, unless the subcontractor submits invoices directly to the CO and COR. This requirement applies to all subcontract types (Cost, FFP, etc.).

13.0 SPECIAL REQUIREMENTS

Not applicable

C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, o person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal #D19-221 Dated 24 June 2019 in response to NAVSEA Solicitation No. N6449819R3504.

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows: (b)(6) and (b)(6) .

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit A through C attached hereto.

CDRL No. Title Data Item Description

A001 Contract Status Report DI-MGMT-81991

A002 Travel Report DI-MISC-81943

A003 Contractor Personnel Roster DI-MGMT-81834A

C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformance's, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be changed to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center

P.O. Box 8000

Corona, CA 92878-8000

Phone: (951) 898-3207

FAX: (951) 898-3250

Internet: http://www.gidep.org

C-227-H009 ACCESS TO DATA OR COMPUTER SOFTWARE WITH RESTRICTIVE MARKINGS (NAVSEA) (JAN 2019)

(a) Performance under this contract may require that the Contractor have access to technical data, computer software, or other sensitive data of another party that contains restrictive markings. If access to such data or software is required or to be provided, the Contractor shall enter into a written agreement with such party prior to gaining access to such data or software. The agreement shall address, at a minimum, (1) access to, and use of, the restrictively marked data or software exclusively for the purposes of performance of the work required by this contract, and (2) safeguards to protect such data or software from unauthorized use or disclosure for so long as the data or software remains properly restrictively marked. In addition, the agreement shall not impose any limitation upon the Government or its employees with respect to such data or software. A copy of the executed agreement shall be provided to the Contracting Officer. The Government may unilaterally modify the contract to list those third parties with which the Contractor has agreement(s).

(b) The Contractor agrees to: (1) indoctrinate its personnel who will have access to the data or software as to the restrictions under which access is granted; (2) not disclose the data or software to another party or other Contractor personnel except as authorized by the Contracting Officer; (3) not engage in any other action, venture, or employment wherein this information will be used, other than under this contract, in any manner inconsistent with this requirement; (4) not disclose the data or software to any other party, including, but not limited to, joint venturer, affiliate, successor, or assign of the Contractor; and (5) reproduce the restrictive stamp, marking, or legend on each use of the data or software whether in whole or in part.

(c) These restrictions on use and disclosure of the data and software also apply to information received from the Government through any means to which the Contractor has access in the performance of this contract that contains restrictive markings.

(d) The Contractor agrees that it will promptly notify the Contracting Officer of any attempt to gain access to any information with restrictive markings. Such notification shall include the name and organization of the individual, company, or Government representative seeking access to such information.

(e) The Contractor shall include this requirement in subcontracts of any tier which involve access to information covered by paragraph (a), substituting "subcontractor" for "Contractor" where appropriate.

(f) Compliance with this requirement is a material requirement of this contract.

C-237-H001 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (NAVSEA) (OCT 2018)

(a) The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the services via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) D, Automatic Data Processing and Telecommunications, IT and Telecom- Telecommunications Transmission (D304) and Internet (D322) ONLY;

(5) S, Utilities ONLY;

(6) V, Freight and Shipping ONLY.

(b) The contractor is required to completely fill in all required data fields using the following web address https://www.ecmra mil.

(c) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://dod.ecmra.support.desk@mail.mil.

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be

notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section J and in the chart listed below:

LIST OF KEY PERSONNEL

Current Key Personnel		
KP Labor Category	**KP Name**	**Date KP Approved**
Manager, Program/Project II	(b)(6)	Modification P0001 (01 June 2020)
Engineer, Systems IV	(b)(6)	Modification P0004 (22 Sept 2020)
Engineer, Systems IV	(b)(6)	Date of Task Order Award
Engineer, Computer IV	(b)(6)	Date of Task Order Award
Engineer, Computer IV	(b)(6)	Date of Task Order Award
Engineer IV	(b)(6)	Date of Task Order Award
Engineer, Systems IV	(b)(6)	Date of Task Order Award
Engineer, Computer IV	(b)(6)	Date of Task Order Award
Information Systems Security Manager II	(b)(6)	Modification P00005 (09 November 2020)
Information Systems Security Manager II	(b)(6)	Modification P00007 (15 March 2021)
Engineer IV	(b)(6)	Modification P00008 (25 March 2021)
Manager, Program/Project II	(b)(6)	Modification P00009 (12 April 2021)
Analyst, Computer Systems III	(b)(6)	Modification P00009 (12 April 2021)
Analyst, Computer Systems III	(b)(6)	Modification P00012 (10 June 2021)
Manager, Program/Project II	(b)(6)	Modification P00013 (01 July 2021)
Information Systems Security Manager II	(b)(6)	Modification P00015 (11 August 2021)
Manager, Program/Project II	(b)(6)	Modification P00016 (29 September 2021)
Information Systems Security Manager II	(b)(6)	Modification P00021 (18 February 2022)
Information Systems Security Manager II	(b)(6)	Modification P00023 (14 April 2022)
Information Systems Security Manager II	(b)(6)	Modification P00023 (14 April 2022)
Substituted Key Personnel		
KP Labor Category	**KP Name**	**Date KP Approved through Removed**
Manager, Program/Project II	(b)(6)	Date of Task Order Award - 01 June 2020
Engineer, Systems IV	(b)(6)	Date of Task Order Award - 22 September 2020
Information Systems Security Manager II	(b)(6)	Date of Task Order Award - 09 November 2020
Engineer IV	(b)(6)	Date of Task Order Award - 25 March 2021
Analyst, Computer Systems III	(b)(6)	Date of Task Order Award - 12 April 2021
Analyst, Computer Systems III	(b)(6)	Date of Task Order Award - 12 April 2021

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contractor's Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: : eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: http://www navsea navy mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft-/ under eCRAFT information. The link for eCRAFT report submission is: https://www.pdrep.csd.disa.mil/pdrep_files/other/ecraft htm. If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification

from eCRAFT.

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

C-242-H002 POST AWARD MEETNG (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within thirty (30) days after award of the Task Order. The meeting will be held at the address below:

Location/Address: *

(b) The contractor will be given at least ten (10) working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the Task Order.

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

[*] Information will be provided by the Contract Specialist/Contracting Officer after Task Order award.

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (OCT 2018)

Notwithstanding FAR 52.244-2(d) and in addition to the information required by FAR 52.244-2(e) of the contract, the contractor shall include the following information in requests to add subcontractors or consultants during performance, regardless of subcontract type or pricing arrangement:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) IF SEAPORT TASK ORDER - The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort contract.